Computer Security Symposium 2017
23 - 25 October 2017

単純なシャッフルを用いた5枚コミット型ANDプロトコル

阿部 勇太[2]　林 優一[3]　水木 敬明[1]　曽根 秀昭[1]

概要：コミット型 AND プロトコルに必要なカード枚数について，ASIACRYPT 2015 にて Koch，Walzer 及び Härtel は，4 枚が必要十分条件であり，有限時間プロトコルに限定した場合には 5 枚が必要十分条件であることを証明した．その十分性の証明には，不均一な確率分布を有するなどの複雑なシャッフルが用いられており，人間が実装することが容易なシャッフルのみを用いて 5 枚以下のコミット型 AND プロトコルを構成できるか否かについては未解決問題とされている．本稿では，人間が容易に実装できるランダムカットとランダム二等分割カットのみを用いて，5 枚のコミット型 AND プロトコルを構成する．このプロトコルは，平均 7 回のシャッフルを使う．

キーワード：カードベース暗号，秘密計算，カード組

1. はじめに

カードベース暗号の研究は，den Boer が 1989 年に考案した Five-Card Trick [1] から始まっている．これは，2 枚の黒いカード ♣ ♣ と 3 枚の赤いカード ♡ ♡ ♡ を使い，論理積 (AND) を秘密計算するものである．ただし，これらのカードの裏面は同一の模様 ? である．本稿は，この Five-Card Trick の紹介から始める．

1.1 Five-Card Trick

AND の秘密計算の入力を与えるために，次の符号化を用いる．

$$\boxed{\clubsuit}\boxed{\heartsuit} = 0, \quad \boxed{\heartsuit}\boxed{\clubsuit} = 1 \tag{1}$$

すなわち，左側に黒いカードが置かれているとき 0 を表し，左側に赤いカードが置かれているとき 1 を表す．この符号化ルール (1) に従い，Alice は 2 枚のカード ♣ ♡ を用いて，自分の秘密の入力ビット $a \in \{0,1\}$ を秘匿した状態で，テーブルの上に置くことができる．

$$\underbrace{\boxed{?}\boxed{?}}_{a}$$

このような裏に置かれた 2 枚のカードは，ビット a の**コミットメント**と呼ばれる．Bob も同様にして，自分の秘密の入力ビット $b \in \{0,1\}$ のコミットメントを（Alice や他の第三者から b の値を秘匿した状態で）テーブルの上に置くことができる．Five-Card Trick [1] は，$a \in \{0,1\}$ と $b \in \{0,1\}$ のコミットメント及び追加カード ♡ を入力として，次の通りに動作する．

(1) 2 つの入力コミットメントの間に追加の赤いカードを置き，a のコメットメントの左右のカードを入れ替えること（NOT 計算）により $\bar{a}$ のコミットメントに変換し，中央の赤いカードを裏返す．

$$\underbrace{\boxed{?}\boxed{?}}_{a}\boxed{\heartsuit}\underbrace{\boxed{?}\boxed{?}}_{b} \rightarrow \underbrace{\boxed{?}\boxed{?}}_{\bar{a}}\boxed{?}\underbrace{\boxed{?}\boxed{?}}_{b}$$

このとき，中央の 3 枚は，$a = b = 1$ のとき，すなわち $a \wedge b = 1$ のときに限り，♡ ♡ ♡ となり，赤 3 枚が連続することに注意しよう．

(2) Alice と Bob はこの 5 枚のカード列に**ランダムカット**（$\langle\cdot\rangle$ で表す）を適用する．

$$\left\langle \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?} \right\rangle \rightarrow \boxed{?}\boxed{?}\boxed{?}\boxed{?}\boxed{?}$$

ランダムカットとは巡回的なシャッフルのことであり，得られるカード列はランダムな数だけシフトしたものとなる．その場にいる誰もが，5 通りの可能性のうち，どの状態であるか分からないよう，人間が安全に実装できることが実験的に確認されている [2]．

(3) 5 枚のカード全てを表にすると，3 枚の ♡ が（巡回的に）連続して並ぶか，そうでないかのどちらかになる．前者の場合 $a \wedge b = 1$ であり，後者の場合 $a \wedge b = 0$ である．

以上が Five-Card Trick であり，非常に単純で誰でも簡

[1] 東北大学サイバーサイエンスセンター
[2] 東北大学工学部
[3] 奈良先端科学技術大学院大学情報科学研究科

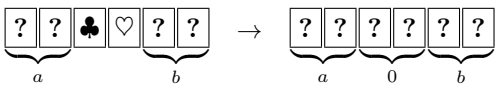
単に AND の秘密計算の実行が可能である．一方，唯一の欠点として，3 入力以上の AND 秘密計算に対応することができない．その欠点を克服するものとして，「コミット型 AND プロトコル」というものが存在し，本稿の主題はそれである．

1.2 6 枚のコミット型 AND プロトコル

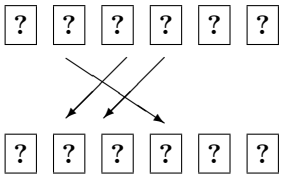
コミット型 AND プロトコルとは，a と b のコミットメント及び何枚かの追加カードを入力として，$a \wedge b$ のコミットメント

を出力するものである．Five-Card Trick と違い，出力がコミットメントとして秘匿された状態で得られるので，出力をそのまま他の計算の入力に使える．これまで数多くのコミット型 AND プロトコルが提案されてきているが，ここでは，その中で人間にとって最も単純で実行が容易な Mizuki-Sone のプロトコル [3] を紹介する．このプロトコルは，2 枚の追加カード ♣ ♡ を用いる．

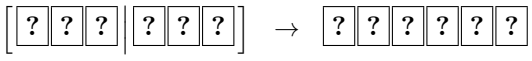
(1) 2 つの入力コミットメントの間に追加カードを置き，裏返す．



(2) 次のように並べ替える．

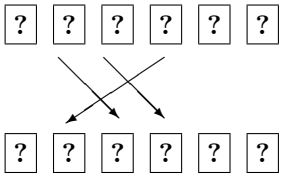


(3) カード列を半分に割り，左右をランダムに入れ替える（これを**ランダム二等分割カット**といい，$[\cdot|\cdot]$ で表す）．

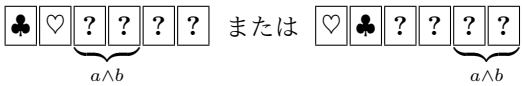


なお，ランダム二等分割カットも，人間が容易に実装できることが示されている [2]．

(4) 次のように並べ替える．



(5) 左側の 2 枚を表にし，♣ と ♡ の並びによって $a \wedge b$ のコミットメントが得られる．



このようなコミット型 AND プロトコルの実行を繰り返すことにより，n 入力 $(x_1, x_2, \ldots, x_n)$ の論理積の秘密計算，すなわち $x_1 \wedge x_2 \wedge \cdots \wedge x_n$ のコミットメントを得ることが可能であることは，すぐに気付くであろう．

1.3 既存の研究と本稿の貢献

いま見たように，コミット型 AND プロトコルの有用性は極めて高く，そのようなプロトコルの設計はカードベース暗号の研究分野の主要なテーマとなっている．実際，表 1 に歴史順に示す通り，数多くのコミット型 AND プロトコルが開発されている．1.2 節で紹介した Mizuki-Sone のプロトコルは，4 番目に登場したものであり，必要なカード枚数が 6 枚と，それまでのプロトコルより少なく，またシャッフルが有限の回数で終了する最初のプロトコルであった．

この 2009 年の Mizuki-Sone の 6 枚 AND プロトコルの登場後，5 枚以下でコミット型 AND プロトコルを構成できるか否かについては，しばらく未解決問題であったが，2015 年に Koch，Walzer 及び Härtel はその解を与えた [4]．すなわち，表 1 に 5 番目のプロトコルとして示している通り，彼らは 4 枚のコミット型 AND プロトコルを与えた．符号化ルール (1) に従う限り，入力コミットメントで 4 枚のカードを必要とするので，このプロトコルはカード枚数が最小という意味で最適である．表 1 に記されている通り，この 4 枚 AND プロトコルは，有限回数のシャッフルでは終了しない．そこで，同時に彼らは，有限回数のシャッフルで終了する 5 枚の AND プロトコルも構成している（表 1 の 6 番目のプロトコル）．さらに彼らは，有限回数のシャッフルで終了する 4 枚のコミット型 AND プロトコルは存在しないことも証明している．従って，有限時間プロトコルに限定した場合，彼らの 5 枚のコミット型 AND プロトコルは（枚数の意味で）最適である．

さて，表 1 を再度眺めてみよう．シャッフルについて「閉じているか？」と「一様分布か？」という列があり，2009 年までの 4 つのプロトコルは，全て「yes」となっていることに気付くであろう．これら 4 つのプロトコルは，ランダムカットあるいはランダム二等分割カットだけを使用している．1.1 節で見たランダムカットは，カードベースプロトコルの厳密な計算モデル [5] に従って記述すると，5 次の対称群 S_5 の要素である恒等置換 id と巡回置換 $\mathsf{sft} = (1\,2\,3\,4\,5)$ を用いて，置換集合

$$\Pi = \{\mathsf{id}, \mathsf{sft}, \mathsf{sft}^2, \mathsf{sft}^3, \mathsf{sft}^4\}$$

とその上の一様分布で表現できる．従って，ランダムカットは “閉じて” おり，“一様” である．同様に，ランダム二等分割カットも一様で閉じている．一方，Koch-Walzer-Härtel のプロトコルで用いられているシャッフルは，表 1 に記載されている通り，閉じていなかったり，一様でなかったり

表 1: コミット型 AND プロトコル

	カード		シャッフル		
	色数	枚数	回数は有限か？	閉じているか？	一様分布か？
Crépeau-Kilian, 1993 [6]	4	10	no	yes	yes
Niemi-Renvall, 1998 [7]	2	12	no	yes	yes
Stiglic, 2001 [8]	2	8	no	yes	yes
Mizuki-Sone, 2009 [3] (§1)	2	6	yes	yes	yes
Koch-Walzer-Härtel, 2015 [4]	2	4	no	yes	no
Koch-Walzer-Härtel, 2015 [4]	2	5	yes	no	no
Ours (§2)	2	5	no	yes	yes

するものが使われている．そのため，人間が実際に実装するのは簡単ではない．

以上ような背景のもと，この研究分野の最も興味深い未解決問題の一つは，次のものである．

> 5 枚以下のカードで，一様で閉じたシャッフルのみを使い，コミット型 AND プロトコルを構成できるか？

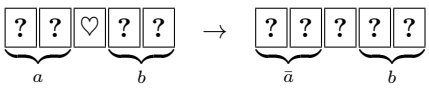
本稿では，この未解決問題を肯定的に解決する．すなわち，5 枚のカードで，一様で閉じたシャッフルのみを使い，コミット型 AND プロトコルを構成する．表 1 の一番下を参照されたい．使用するシャッフルは，ランダムカットとランダム二等分割カットのみであり，上述の通りどちらも人間が容易に実装できるので，提案するプロトコルは人間が実際に実行することが可能である．

2. プロトコル

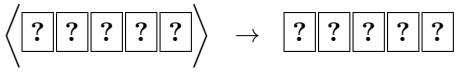
本節では，5 枚のコミット型 AND プロトコルを提案する．

このプロトコルは，次に記す通り，最初は途中まで Five-Card Trick と同様な手順を適用し，その後，ランダムカットやランダム二等分割カットを用いて，論理積のコミットメントを出力する．

(1) Five-Card Trick のステップ (1) を行う．



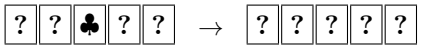
(2) Five-Card Trick のステップ (2) を行う．



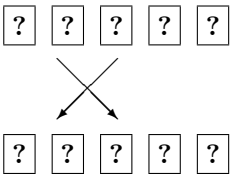
を行う．

(3) 中央の 1 枚を表にする．♡ が出たら，そのカードを裏にしてからステップ (2) に戻る．♣ が出たら，次のステップに進む．（♣ が出る確率は 2/5 である．）

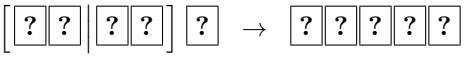
(4) 中央の ♣ を裏にし，



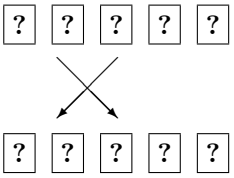
並べ替える．



(5) 左からの 4 枚に対しランダム二等分割カットを適用する．

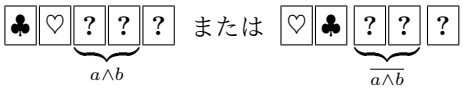


(6) 並べ替える．

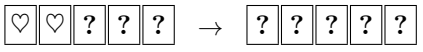


(7) 左から 2 枚をめくる．

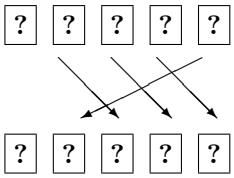
(a) ♣♡ あるいは ♡♣ が出たら，$a \wedge b$ のコミットメントが得られる．



(b) ♡♡ が出たら，これらを裏にし，



並べ替え，



ステップ (2) へ戻る．（この ♡♡ が出る確率は 1/2 である．）

以上が提案コミット型 AND プロトコルである．プロトコル中にはループを含んでいるため，有限の回数のシャッフルでは終了しないが，シャッフルの回数の期待値は 7 回と計算できる．

疑似コード風にこのプロトコルを記述すると，次の通り

となる．

---

input set:

$$\left\{\left(\frac{?}{\clubsuit},\frac{?}{\heartsuit},\frac{\heartsuit}{?},\frac{?}{\clubsuit},\frac{?}{\heartsuit}\right),\left(\frac{?}{\clubsuit},\frac{?}{\heartsuit},\frac{\heartsuit}{?},\frac{?}{\heartsuit},\frac{?}{\clubsuit}\right),\right.$$
$$\left.\left(\frac{?}{\heartsuit},\frac{?}{\clubsuit},\frac{\heartsuit}{?},\frac{?}{\clubsuit},\frac{?}{\heartsuit}\right),\left(\frac{?}{\heartsuit},\frac{?}{\clubsuit},\frac{\heartsuit}{?},\frac{?}{\heartsuit},\frac{?}{\clubsuit}\right)\right\}$$

(perm, (1 2))
(turn, {3})
1 (shuf, {id, sft^1, sft^2, sft^3, sft^4})
(turn, {3})
if visible seq. = (?, ?, ♡, ?, ?) **then**
(turn, {3})
goto 1
(perm, (2 3))
(shuf, {id, (1 3)(2 4)})
(perm, (2 3))
(turn, {1, 2})
if visible seq. = (♡, ♡, ?, ?, ?) **then**
(turn, {1, 2})
(perm, (2 3 4 5))
goto 1
if visible seq. = (♣, ♡, ?, ?, ?) **then**
(result, 3, 4)
if visible seq. = (♡, ♣, ?, ?, ?) **then**
(result, 4, 3)

---

3. おわりに

本稿では，人間が容易に実装できるランダムカットとランダム二等分割カットのみを用いて，5 枚のコミット型 AND プロトコルを構成し，未解決問題 [4], [9] を解決した．

参考文献

[1] den Boer, B.: More Efficient Match-Making and Satisfiability: the Five Card Trick, *Advances in Cryptology — EUROCRYPT '89* (Quisquater, J.-J. and Vandewalle, J., eds.), Lecture Notes in Computer Science, Vol. 434, Springer Berlin Heidelberg, pp. 208–217 (online), DOI: 10.1007/3-540-46885-4_23 (1990).

[2] Ueda, I., Nishimura, A., Hayashi, Y.-i., Mizuki, T. and Sone, H.: How to Implement a Random Bisection Cut, *Theory and Practice of Natural Computing* (Martín-Vide, C., Mizuki, T. and Vega-Rodríguez, M. A., eds.), Springer International Publishing, Cham, pp. 58–69 (online), DOI: 10.1007/978-3-319-49001-4_5 (2016).

[3] Mizuki, T. and Sone, H.: Six-Card Secure AND and Four-Card Secure XOR, *Frontiers in Algorithmics* (Deng, X., Hopcroft, J. E. and Xue, J., eds.), Lecture Notes in Computer Science, Vol. 5598, Springer Berlin Heidelberg, pp. 358–369 (online), DOI: 10.1007/978-3-642-02270-8_36 (2009).

[4] Koch, A., Walzer, S. and Härtel, K.: Card-Based Cryptographic Protocols Using a Minimal Number of Cards, *Advances in Cryptology - ASIACRYPT 2015* (Iwata, T. and Cheon, J. H., eds.), Lecture Notes in Computer Science, Vol. 9452, Springer Berlin Heidelberg, pp. 783–807 (online), DOI: 10.1007/978-3-662-48797-6_32 (2015).

[5] Mizuki, T. and Shizuya, H.: A formalization of card-based cryptographic protocols via abstract machine, *International Journal of Information Security*, Vol. 13, No. 1, pp. 15–23 (online), DOI: 10.1007/s10207-013-0219-4 (2014).

[6] Crépeau, C. and Kilian, J.: Discreet Solitary Games, *Advances in Cryptology — CRYPTO '93* (Stinson, D. R., ed.), Lecture Notes in Computer Science, Vol. 773, Springer Berlin Heidelberg, pp. 319–330 (online), DOI: 10.1007/3-540-48329-2_27 (1994).

[7] Niemi, V. and Renvall, A.: Secure multiparty computations without computers, *Theoretical Computer Science*, Vol. 191, No. 1–2, pp. 173–183 (online), DOI: 10.1016/S0304-3975(97)00107-2 (1998).

[8] Stiglic, A.: Computations with a deck of cards, *Theoretical Computer Science*, Vol. 259, No. 1–2, pp. 671–678 (online), DOI: 10.1016/S0304-3975(00)00409-6 (2001).

[9] Koch, A. and Walzer, S.: Foundations for Actively Secure Card-based Cryptography, Cryptology ePrint Archive, Report 2017/422 (2017).